Law Office of Brian J. Levine

75 NORTH BRIDGE STREET
SOMERVILLE, NEW JERSEY 08876
Phone: (908) 243-0111 Fax: (908) 243-0222

www.bllawnj.com
blevine@bllawnj.com

BRIAN J. LEVINE *
LISA PEZZANO MICKEY [1]
(Of Counsel)

* Certified by the Supreme Court of
New Jersey as a Civil Trial Attorney

[1] Also Admitted in New York

January 31, 2022

Hon. Tonianne J. Bongiovanni, U.S.M.J.
Clarkson S. Fisher Federal Building
and U.S. Courthouse
402 E. State Street
Trenton, New Jersey 08608

Re: *UMG Recordings, Inc. et al. v. RCN Telecom Services, LLC et al.*,
Civil Action No. 19-17272 (MAS) (TJB)

Dear Judge Bongiovanni:

This firm, along with Steptoe & Johnson, represents counterclaim-defendant Rightscorp, Inc. ("Rightscorp") in the above-referenced action. Pursuant to Local Civil Rule 37.1(a)(1), we submit this letter in response to the December 30, 2021 discovery dispute letter filed by Defendants and Counterclaimant RCN Telecom Services, LLC, *et al.* ("RCN") (ECF 195). First, RCN demands to be given unfettered and onsite access to the full Rightscorp system. As explained below, this overreaching request should be denied because (a) RCN has failed to even request such sweeping access; (b) Rightscorp has produced to RCN the source code which explains in full how the system was designed, how it works and what it does, together with files containing data relevant to the rampant infringement taking place on RCN's network; and (c) the significant burden on Rightscorp and risk to its live infringement detection system if RCN and its experts are handed the keys to the entire system for days at a time. RCN has not established why the source code and data files provided (together with substantial prior deposition testimony of Rightscorp personnel) is insufficient. Indeed, RCN even rejected Rightscorp's offer (made *four months ago*) to provide RCN with a copy of its database containing RCN only data. The answer is simple—RCN wants to fish around in the hopes of finding something that the source code, data sets, emails, prior deposition testimony and more has not yet revealed.

Second, RCN demands that Rightscorp serve initial disclosures in response to RCN's counterclaim. As noted below, that patently frivolous counterclaim already has been dismissed once and is subject to a second pending motion to dismiss. Rightscorp will, of course, provide such disclosures if the pending motion is denied, but there is no valid reason why it needs to incur the costs and burden of preparing a response at this time. Tellingly, RCN is trying to hold Rightscorp to a standard that RCN itself has not met, *as RCN has never served Rightscorp with its own initial disclosures prepared in response to Plaintiffs' claims or amended those disclosures to account for its counterclaim.*

RCN's letter regarding Rightscorp is pretextual and is a blatant attempt to deflect the focus of this action away from RCN's manifest liability for the massive copyright infringement alleged in the Amended Complaint. This case is about RCN and the substantial infringement that takes place unchecked on its system, not Rightscorp. RCN's letter request should be denied in full.

BACKGROUND

Rightscorp developed and employs a proprietary technology to monitor copyright infringements occurring on the online peer-to-peer network known as BitTorrent. Specifically, Rightscorp's technology identifies when BitTorrent users make certain copyrighted content available for distribution, documents those acts of copyright infringement, and then notifies the internet service providers ("ISPs") who provide broadband service to those BitTorrent users of the infringements being committed by their subscribers. In this lawsuit, Plaintiffs rely on Rightscorp's reports of infringement and supporting information to support their claims of copyright infringement asserted against RCN. During the discovery process, Plaintiffs have provided RCN with extensive information concerning Rightscorp, including: the source code underlying Rightscorp's software; millions of infringement notices that Rightscorp sent to RCN; infringing audio files downloaded by Rightscorp from users of RCN's network; data associated with the infringements Rightscorp detected; numerous other internal and external Rightscorp documents; and transcripts of multiple depositions of Rightscorp's personnel from other actions. This information demonstrates that users of RCN's network infringed Plaintiffs' copyrights and that RCN was made aware of that infringement.

To be clear, Rightscorp is not a proper party to this action: it is an independent third party that provided reports of infringement and related information to Plaintiffs, who own the sound recording copyrights at issue in this case. Indeed, the only reason Rightscorp is a party in this dispute is because RCN filed a frivolous counterclaim against Plaintiffs and included Rightscorp as an additional counterclaim-defendant. Judge Shipp dismissed that claim, but permitted RCN to attempt to replead it. That amended pleading is currently subject to Rightscorp's and Plaintiffs' pending motions to dismiss. Nevertheless, recognizing the devastating impact of Rightscorp's reports and supporting information, the absence of any good faith defense to the claims asserted, and the need to shift attention away from its own conduct, RCN has sought burdensome, disproportionate and intrusive discovery from Rightscorp that is unwarranted whether or not Rightscorp remains as a party to this action.

In their prior submissions concerning discovery disputes, Rightscorp and Plaintiffs have provided the Court with the factual background concerning Rightscorp's detection of online peer-to-peer copyright infringement on RCN's network. *See* ECF 171, 172, 194. In summary, Rightscorp's technology detects infringement of music, movies, television shows and other media content by internet users of peer-to-peer file sharing technologies, most notably BitTorrent. Rightscorp captures data concerning such infringement and generates notices that it sends to ISPs, identifying the infringing activity and the IP address at which the infringement occurred, so that the ISPs can notify their subscribers that such activity is unlawful and take action to stop further unlawful activity, including terminating repeat infringing subscribers.

This is not the first time that Rightscorp's online infringement detection system and the information it captures has been the basis for litigation by copyright holders. In other cases against ISPs, Rightscorp's data has been deemed reliable: it has supported multiple favorable court rulings and a favorable jury verdict for copyright infringement.[1] With regard to the allegations of this case, Rightscorp has detected and sent RCN millions of notices since 2011 concerning instances of online infringement by RCN network users. Rightscorp also has downloaded at least one infringing copy of each of Plaintiffs' sound recordings that are the works in suit directly from RCN subscribers.

ARGUMENT

I. THERE IS NO BASIS FOR RCN'S EXTRAORDINARY DEMAND THAT IT BE GIVEN UNFETTERED ACCESS TO INSPECT RIGHTSCORP'S COMPUTER SYSTEM.

A. RCN has never served a request to enter Rightscorp's premises and inspect its computer system.

RCN's letter expressly seeks direct "access for RCN's counsel and technical expert" to inspect Rightscorp's "servers and databases." ECF 195 at 2. However, RCN has never served a

[1] *See BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc.*, 149 F. Supp. 3d 634 (E.D. Va. 2015) (summary judgment) and 199 F. Supp. 3d 958 (E.D. Va. 2016) (post-trial motions) (crediting the "significant evidentiary value" of Rightscorp's infringement notices in supporting the jury verdict), *aff'd in part and rev'd in part on other gounds*, 881 F. 3d 293 (4th Cir. 2018); *UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC*, 384 F. Supp. 3d 743, 757-58 (W.D. Tex. 2019) (in case against RCN's sibling company, finding Rightscorp data necessitated jury trial and rejecting various challenges to Rightscorp's system).

discovery request to go onto Rightscorp's property and inspect its computer systems. For that reason alone RCN's request should be denied.

It is axiomatic that "before a party may succeed on a motion to compel discovery, that party 'must first prove that it sought discovery' in the manner required by the rules of procedure." *Camiolo v. State Farm Fire and Cas. Co.*, 334 F.3d 345, 360 (3d Cir. 2003) (quoting *Petrucelli v. Bohringer and Ratzinger*, 46 F3d. 1298, 1310 (3d Cir. 1995)) (district court did not abuse discretion in denying motion to compel where no formal request complying with the Federal Rules sought the discovery to be compelled). Moreover, as relevant here, Rule 34 distinguishes between discovery requests "to permit entry onto designated land or other property possessed or controlled by the responding party" and requests to "produce" documents. *Compare* Fed. R. Civ. P. 34(a)(1) and (a)(2).

RCN fails to cite and in fact never served a discovery request seeking to inspect Rightscorp's computer systems. The only discovery request that RCN cites is Request for Production No. 3. *See* ECF 195 at 3. However, that request plainly did not seek the extraordinary discovery (an unfettered multi-day inspection of Rightscorp's computer system) that RCN now seeks to compel. Instead, it merely sought the production of documents and electronically stored information. *See* ECF 195-5 at 8-9.[2] Indeed, although RCN and its counsel are very familiar with the Rightscorp computer system from their work on the Grande case, have deposed Rightscorp witnesses at length about the Rightscorp computer system, and have had access to the Rightscorp source code for years, their discovery requests did not specifically mention the Rightscorp database, much less seek to inspect Rightscorp's computer systems.

RCN's clear failure to serve a formal discovery request seeking entry onto Rightscorp's premises is not an academic point. Rather, it reflects RCN's imprecise and shifting tactics with regard to obtaining discovery from Rightscorp. As noted above, the discovery request at issue seeks documents and ESI "obtained from a user of RCN's network." ECF 195-5 at 8. During the meet and confer process, however, RCN took the position that this request encompassed Rightscorp's native database. Specifically, on April 7, 2021, counsel for RCN asked that "Rightscorp make available for *copying* the database(s) that collect information obtained by its system, which is separate from any source code." ECF 195-2 at 2 (Apr. 17, 2021 Howenstine email to Newberg) (emphasis added). Although Rightscorp believed that production of its source code and the massive amount of other supporting documentation was more than sufficient for RCN to assess the Rightscorp system, it conferred in good faith with RCN in an effort to resolve the dispute. These discussions culminated in Rightscorp's making a compromise proposal: Rightscorp offered to "create a duplicate copy of the native database that includes only information related to

[2] RCN's Request for Production No. 3 to Rightscorp sought: "All Documents and Things, including without limitation all electronically-stored information in any form whatsoever, obtained from a user of RCN's network, including without limitation all bitfield, choke, have, and request data."

RCN." ECF 195-4 at 2-3 (Sept. 17, 2021 Allan email to Howenstine). This offer should have resolved the dispute, as it plainly satisfied RCN's request for a copy of the database, at least with respect to data obtained from users of RCN's network. But without justification, RCN rejected this proposal and moved the goalposts again, insisting that a copy no longer was sufficient and that it now wanted to "examine" Rightscorp's systems "in full" via "inspection[] at Rightscorp's offices." *Id.* at 1 (Sept. 22, 2021 Howenstine email to Allan). Even putting aside that RCN never served a request for access to Rightscorp's premises, that demand exceeds the scope of RCN's document request, as it seeks access to (a) information related to users of other networks besides RCN's and (b) information that is not obtained from any user of any network at all. Accordingly, during subsequent meet and confer discussions, counsel for Rightscorp rejected RCN's demand.

After Rightscorp rejected RCN's demand, RCN let more than *three months* pass before raising this issue again, without warning, as part of its December 30, 2021 discovery letter.[3]

Like any litigant, RCN should be held to the discovery request it actually served and not be permitted to use its requests as starting points to demand broader discovery. If RCN truly thought that an inspection was necessary, it would have served a request for one, and would have pursued relief from the Court in a more timely manner. RCN's failure to do so is, standing alone, a sufficient reason to deny RCN's application.[4]

B. RCN fails to provide any valid reason why an on-site inspection of Rightscorp's computer system is necessary.

RCN has not made its request for an on-site inspection on a blank slate. In response to RCN's document requests, Plaintiffs and Rightscorp have already produced a massive volume of documents and data concerning Rightscorp's detection of infringement on RCN's network, including the following:

- The Rightscorp technology computer source code (including periodic updates to that code implemented over time). Importantly, the source code contains the specific technical details as to how the Rightscorp system works to detect copyright infringement and notify ISPs, like RCN, of that infringement;

[3] For purposes of this letter, Rightscorp understands that RCN now seeks "access to the SQL server and related database or databases that Rightscorp used and uses to store data obtained from individual BitTorrent users, through the operation of its system for detecting and notifying ISPs of alleged copyright infringements." ECF 195 at 3 n.2.

[4] Consistent with both RCN's discovery requests and its letter to the Court, Rightscorp remains willing to produce a duplicate copy of its database containing the information it obtained from users of RCN's network through the operation of its system for detecting and notifying ISPs of copyright infringement.

- 4,665,884 email notices of copyright infringement by users of RCN's internet service;
- 314,440 emails that RCN sent to Rightscorp regarding Rightscorp's email notices;
- 808 "Dashboard" summaries of infringement activity on RCN's network;
- 56,267 infringing files downloaded from RCN internet users;
- Three large database files generated from the vary database RCN seeks to access, that contain the data associated with the email notices and downloaded files;
- Data associated with an additional 1.4 million instances of infringement detected on RCN's network;
- 2,709 other Rightscorp documents (emails, spreadsheets, presentations); and
- A detailed log identifying documents Rightscorp has withheld on privilege and work product grounds.

This information is more than sufficient to satisfy RCN's document requests and its discovery needs in this case.[5] Indeed, RCN utterly fails to explain why its informal request for an on-premises, unfettered inspection of Rightscorp is justified. The Advisory Committee Notes to Rule 34 caution that the rule "is not meant to create a routine right of direct access to a party's electronic information system" and that "[c]ourts should guard against undue intrusiveness resulting from inspecting or testing such systems." Adv. Cmte Notes, 2006 Amendment to Rule 34. Consistent with this cautionary statement, courts since the 2006 amendment to Rule 34 have emphasized that "mere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures." *John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008) (citing *McCurdy Group, LLC v. Am. Biomedical Group, Inc.*, 9 F. App'x 822, 831 (10th Cir. 2001)). No less than the Sedona Conference has noted that "[c]ivil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail."[6] Thus, "courts are not inclined to

[5] The materials that Rightscorp has already produced to RCN clearly refute RCN's claim that its requested inspection of Rightscorp's system is "highly relevant to understanding how Rightscorp's system operates." ECF 195 at 1. RCN and its counsel are well aware of how the Rightscorp system operates: they have Rightscorp's source code (which is effectively the instructions for the system), data maintained by Rightscorp's system about the infringements at issue (which were generated as a result of that source code), and testimony from Rightscorp's employees describing how the Rightscorp system operates. Tellingly, in Plaintiffs' parallel case against Grande Communications (RCN's sibling ISP, represented by the same counsel that represents RCN here), and in the *BMG v. Cox* case, no party ever requested the type of access RCN now seeks in order to evaluate the infringement claims at issue. In those cases, Rightscorp produced the same level of documents and data (or less) than is already available to RCN.

[6] Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, Second Edition 11, 28 (The Sedona Conference Working Group Series, 2007), at 34, 37, *available at* http://www. thesedonaconference.org/content/miscFiles/ TSC_PRINCP_2nd_ed_607.pdf.

compel such discovery unless, for example, suspicious discrepancies exist in a party's production, or the party has consistently failed to produce relevant information." *Aster Rsch. Techs., Inc. v. Raba-Kistner Infrastructure, Inc.*, No. SA-07-CA-93-HLH, 2009 WL 10701166, at *8 (W.D. Tex. July 8, 2009) (citation omitted).

Here, RCN falls far short of justifying an on-site inspection of Rightscorp's computer system. In its letter, RCN sets forth two supposed categories of information that it seeks to obtain through on-site inspection. Neither category warrants entry onto Rightscorp's premises.[7]

The first category RCN discusses is data that RCN claims could have been collected from BirTorrent users, most notably "bitfield" and "choke" data. ECF 195 at 3. This argument is not asserted in good faith because RCN knows full well that Rightscorp's infringement detection system was not designed to maintain this information. If it had been, there would be evidence of that design in Rightscorp's source code. However, despite having access to Rightscorp's source code, RCN does not cite to the source code to support its request—undoubtedly because the source code affirmatively reveals that its system does *not* maintain the data RCN seeks. This precise issue was previously addressed in *Grande*, where that court denied a spoliation motion brought by the defendant (again, RCN's sibling company, represented by RCN's counsel). *See UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC*, No. A-17-CA-365-LY, 2019 WL 4738915, at *4 (W.D. Tex. Sept. 27, 2019). RCN's one-sentence characterization of this ruling (*id.* at 5) is misleadingly incomplete: the *Grande* court correctly observed that Rightscorp's system considers some of this data when determining whether to send notices to ISPs, but is not designed to maintain that data in its database. *See id.*[8] Thus, even if RCN were to obtain the relief it requests, it would not find the data it claims to seek. RCN knows this, but fails to mention it to the Court.

The second category RCN claims to seek is the "relational database that allows the user to retrieve and organize all available information related to a data entry." ECF 195 at 4. However, Rightscorp offered to make such information available to RCN months ago. RCN does not and

[7] Tellingly, the only case that RCN cites concerning forensic inspection did not concern a request for on-site inspection. *See Lux Glob. Label Co., LLC v. Shacklett*, No. 2:18-cv-5061, 2020 WL 1700572 (E.D. Pa. Apr. 8, 2020). There, a party sought access to specific electronic devices and online accounts so they could be forensically imaged by a neutral third-party vendor. *See id.* at *3-4. Nothing in that case addressed a request made by one party to enter another party's premises and access its electronic systems directly.

[8] In particular, the court recognized that while Rightscorp's software considers bitfield data when it evaluates BitTorrent users to determine whether they are offering infringing files, the Rightscorp system "simply never intended, and was not designed, to retain" such data. *Grande*, 2019 WL 4738915, at *4. Further, Rightscorp's software "does not make use" of choke data or the other types of data RCN references, "and thus there is no reason why it would retain any of that data." *Id.*

cannot explain why the copy of the native database that Rightscorp previously offered—with data limited to that obtained from users of RCN's network—would not satisfy RCN's claimed needs. Indeed, that copy would contain all the "relational" information that is available about the infringements underlying the notices Rightscorp sent to RCN, which RCN could verify by comparing the database copy to the source code that has already been produced. Instead, RCN complains that it should not have to rely on the accuracy of that copy of the database. However, even that inadequate response is based on nothing more than the unsupported, self-serving allegations of RCN's counsel. RCN's "mere skepticism" that the copy of the native database will contain the information it seeks is manifestly baseless and falls far short of a showing that would justify the extraordinary relief requested, particularly given the enormous volume of Rightscorp-related information already produced in discovery and the litigation track record concerning the reliability of the Rightscorp system. *John B.*, 531 F.3d at 460.[9]

C. The intrusive on-site inspection RCN seeks would be prejudicial to Rightscorp.

RCN's requested relief would also harm Rightscorp's ongoing business operations. Rightscorp is actively operating its infringement detection technology: it is running its software, detecting infringement online, sending notices about that infringement to ISPs, and downloading infringing files from BitTorrent users. All of that would need to cease to allow RCN's lawyers and experts to sit onsite at Rightscorp and rifle through its computer systems. Moreover, given that Rightscorp's system is live, inadvertent key strokes by RCN's lawyers or experts could delete information, or otherwise create changes in the system or database, and generate massive problems for Rightcorp.

RCN does not even try to explain how the intrusive, days-long onsite inspection it proposes possibly could be accommodated by Rightscorp without significant disruption to Rightscorp's business. Nor does RCN explain how it would refrain from accessing data concerning *other* ISPs besides RCN, or other aspects of Rightscorp's IT systems beyond the data relevant to this case—likely because RCN knows that such segregation would not be feasible (at least not without significant logistical hurdles) if it is on-site and accessing Rightscorp's system directly. The Advisory Committee comments and relevant case law discussed above all confirm that a party seeking direct, on-premises, access to ESI must show that its need for this sort of intrusive discovery outweighs the resisting party's concerns about confidentiality, business disruption, and cost. RCN barely addresses these issues, let alone persuades that the balancing tilts at all in its favor.

[9] RCN also argues that inspection of the databases is justified because Rightscorp was "sanctioned" in one case and "accused" of spoliation in another case. *See* ECF 195 at 5. These claims lend no support to RCN's request here. In the first case (*Cox*), the "sanction" was a simply a jury instruction and was based on the lack of a version control system, no longer at issue; in the latter case (*Grande*), the accusation, which was made by the same lawyers who represent RCN in this case, was rejected by the court.

* * *

In sum, RCN has failed to justify its extraordinary request for an on-site inspection of Rightscorp's computer system. Rightscorp has already produced a huge volume of documents and data to RCN and has offered to produce a native copy of the relevant portions of its database, satisfying both RCN's actual requests before it moved the goal posts and RCN's purported reasons for wanting the information. RCN is not entitled to more.

II. Rightscorp Should Not Be Compelled To Serve Initial Disclosures Responding To RCN's Counterclaim Unless and Until RCN Itself Provides Amended Initial Disclosures And The Court Sustains RCN's Counterclaim.

As noted above, Rightscorp is plainly not a proper party to this case. As nothing more than a litigation tactic, RCN concocted a counterclaim as a basis to name Rightscorp as a defendant, claiming that Rightscorp's operation of its technology to detect and notify ISPs about copyright infringement on their networks somehow amounts to "unfair competition" under California's Unfair Competition Law ("UCL"). Rightscorp filed a motion to dismiss RCN's original counterclaim, as did Plaintiffs and their trade association, the Recording Industry Association of America ("RIAA"), whom RCN also named as counterclaim-defendants. The Court ***granted*** those motions on June 30, 2021. *See* ECF 159 & 160. RCN filed an amended counterclaim on July 20, 2021. Because RCN's amended counterclaim suffers from the same (incurable) legal and factual defects as the original counterclaim, Rightscorp, Plaintiffs, and the RIAA all filed renewed motions to dismiss. *See* ECF 174 & 175. Those motions to dismiss are pending.

RCN's baseless counterclaim is the only reason RCN now insists that Rightscorp should serve initial disclosures. But Rightscorp should not be required to provide initial disclosures until this Court has ruled on its motion to dismiss RCN's counterclaim. RCN appears to have raised this issue for the sole purpose of making misleading and irrelevant allegations about Rightscorp.[10] *See* ECF 195 at 6. RCN offers no reason why it needs Rightscorp's disclosures now.

Moreover, RCN's complaint about Rightscorp's initial disclosures is hypocritical. RCN itself has not served Rightscorp with its initial disclosures or, more importantly, amended those disclosures to identify any relevant information that it would use to support its counterclaim. Having failed to provide initial disclosures to Rightscorp, RCN cannot legitimately complain about Rightscorp's doing the same.

[10] RCN insinuates that Rightscorp is not a validly incorporated going concern. Not only is that accusation meritless, but it has no relevance to whether Rightscorp should be required to serve initial disclosures. (It bears emphasis that Rightscorp has fully participated in the conduct of this litigation, including motions and written discovery responses, all signed and served by counsel as officers of the Court.)

Accordingly, Rightscorp submits that it should not be required to serve initial disclosures unless and until (1) RCN itself has served its amended disclosures, and (2) the Court denies the counterclaim-defendants' renewed motions to dismiss.

Respectfully submitted,

s/Brian J. Levine

BRIAN J. LEVINE

BJL/pct
cc: Edward F. Behn, Jr., Esq.
Richard L. Brophy, Esq.
Zachary C. Howenstine, Esq.
Margaret R. Szewczky, Esq.
Kyle Gottuso, Esq.